Fortinet Customer Configuration Guide

Adentro Overview

Adentro provides consumers with an amazing WiFi experience at their favorite spots, while helping to grow local businesses by better engaging and targeting their customers. By offering a branded captive portal for your guest WiFi network, customers are given the ability to opt-in to targeted messaging sent using the Adentro platform.

Adentro supports the following Fortinet Hardware:

- FortiGate 60E or 60D running a firmware version of 6.0.4 or newer
    - FortiAP 221E or compatible

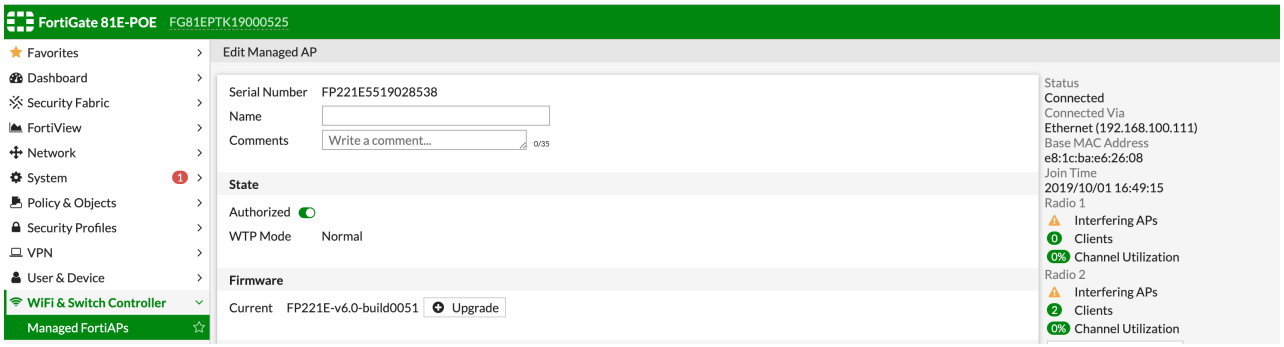
Adentro Configuration

In order to associate your Fortinet access point(s) with your business location, Adentro will need the MAC address of each individual access point that will be broadcasting the integrated SSID. You can find this information on the back of the access point or in the FortiGate management interface.

To find the AP Mac address(es) in the Fortigate management interface:

1. Select "Managed FortiAPs" under "WiFi & Switch Controller"
2. Edit the AP.

You will see the client mac under "Base MAC Address" to the right of the screen.



Record all AP MAC addresses and forward it to your Adentro Account Manager. Without completion of this step for all APs, guests will receive a "404" error on the captive portal. Adentro will respond by giving you two secrets (RADIUS and Presence) that you will need to complete the captive portal setup.

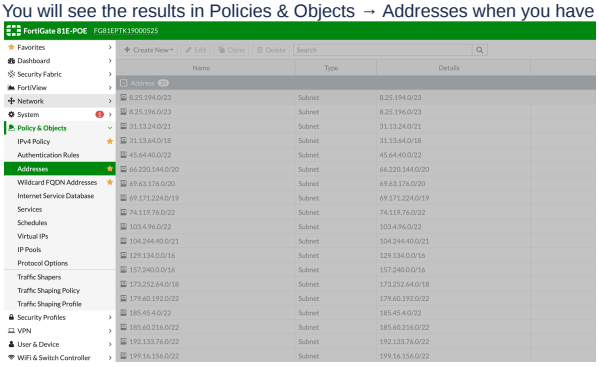
Fortinet Configuration

All configuration takes place in the Fortigate management interface (either local or cloud).

Step 1: Created Walled Garden Address Groups

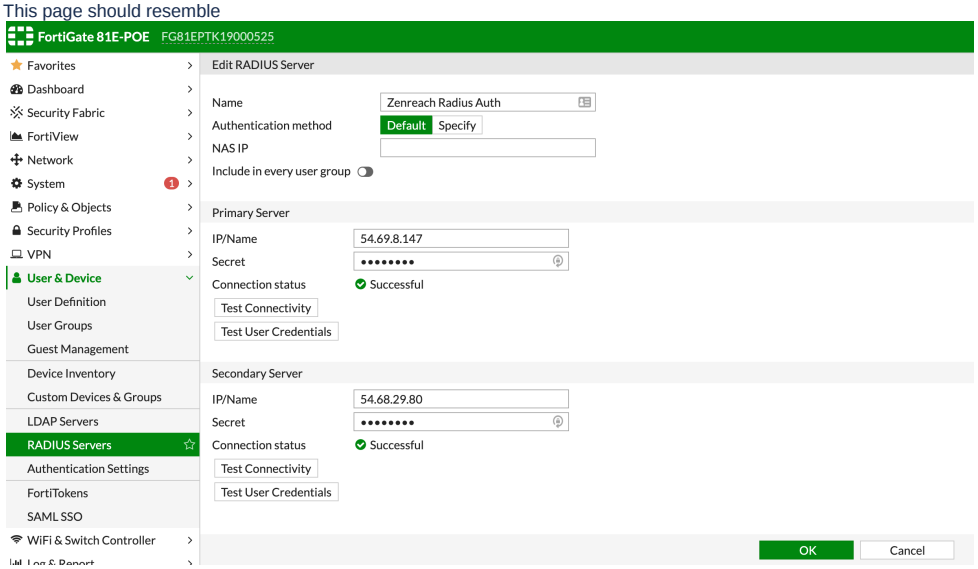
This is very cumbersome and error prone in the UI, so instead run the following commands in the CLI to configure the addresses you will need in the walled garden:

You will see the results in Policies & Objects → Addresses when you have completed the CLI commands above:



Step 2: Setup Adentro Radius Auth and Accounting

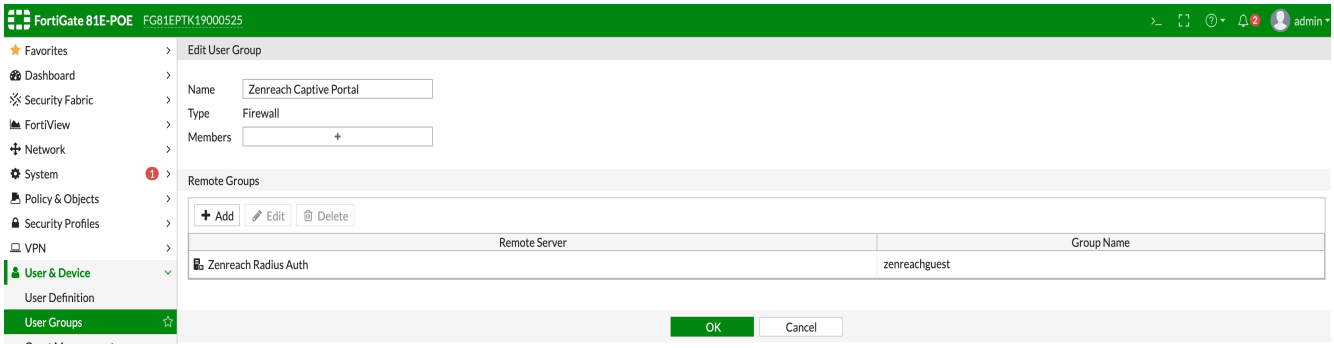
1. In the code snippet below replace **<SECRET>** with the secret that was provided to you by Adentro when you gave us your access point mac address.
2. Paste and run the updated code block into console
3. Navigate to User & Device > RADIUS Servers
4. This page should resemble



5. Click "Test Connectivity" buttons for both primary and secondary to confirm it works.

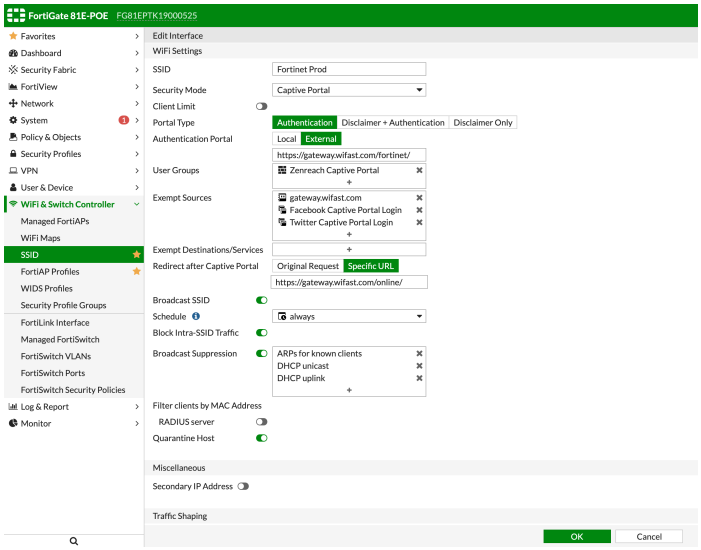
Step 3: Set up the Adentro Captive Portal Group

1. Navigate to User & Device > User Groups and click Create New
2. Enter the following information:
   Name: Adentro Captive Portal
   Type: Firewall
3. Click the "Add" button and pick
   a. "Zenreach Radius Auth" as the RADIUS Server
   b. Toggle group to specify
   c. Add "zenreachguest" as the Group Name.
4. It should like like below when complete. Then click "OK" to save.



Step 4: Set up the Captive Portal

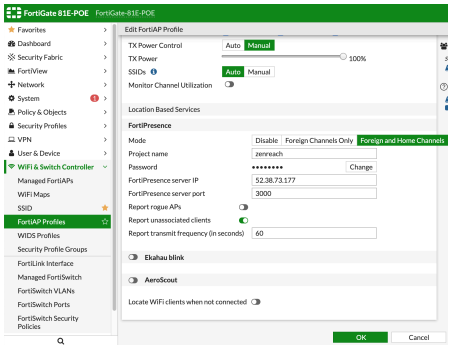
1. Log into the Fortigate Management Interface
2. In the left menu, click "WiFi & Switch Controller" and then SSID.
3. Scroll down to the "WiFi Settings" section and enter the following information:
   SSID: <Pick a name for your SSID>
   Security Mode: Captive Portal
   Portal Type: Authentication
   Authentication Portal: Pick "External" and then enter the following in the text box below it: "https://gateway.wifast.com/fortinet/"
   User Groups: Pick "Zenreach Captive Portal"
   Redirect after Captive Portal: https://gateway.wifast.com/online/
   Exempt Destinations: gateway.wifast.com, "Facebook Captive Portal Login", "Twitter Captive Portal Login"
4. Click "Ok" to save your SSID changes



Step 5: Set up FortiPresence

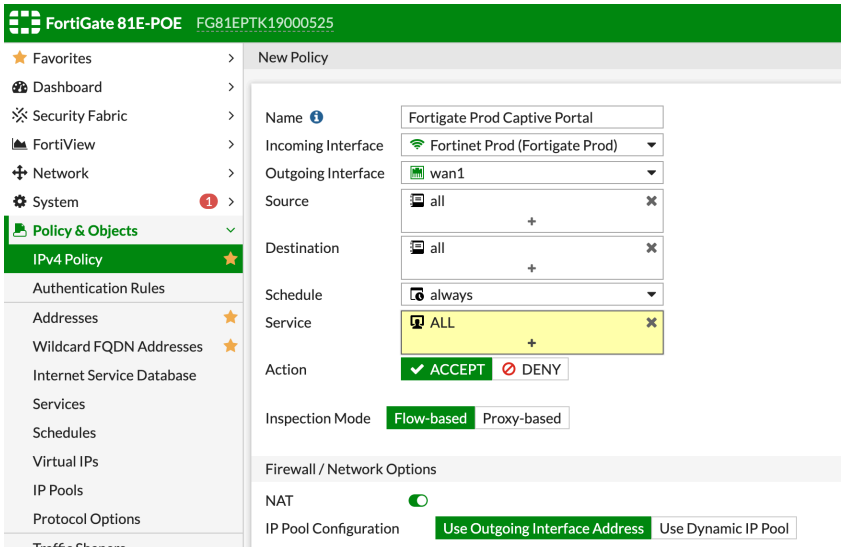
It is critical to set up the FortiPresence interface to detect customer visits even if no captive portal login occurs. Do this by:

1. Selecting "WiFi & Switch Controller" and then "FortiAP Profiles" from the left menu.
2. Scroll down to the "FortiPresence" section and set the following options:
   Mode: Foreign and Home Channels
   Project Name: zenreach
   Password: <Adentro will issue you one when you inform them of your access point mac address>
   FortiPresence server IP: 52.38.73.177
   FortiPresence server port: 3000
   Report rogue APs: Unchecked
   Report unassociated clients: Checked
   Report Transmit Frequency: 60
3. Click "Ok" to save your changes.



Step 6: Set up Firewall policy for captive portal

1. Navigate to Policy & Objects > IPv4 Policy and click "Create New"
2. Set the following fields and then press "OK" to save:
   Name: <Pick a name>
   Incoming Interface: <Pick your Captive Portal>
   Source: all
   Destination: all
   Schedule: always
   Service: ALL
   Action: ACCEPT
   Inspection Mode: Flow-based
   NAT: Enabled


FortiGate 81E-POE
FG81EPTK19000525
Favorites
Dashboard
Security Fabric
FortiView
Network
System
1
Policy & Objects
IPv4 Policy
Authentication Rules
Addresses
Wildcard FQDN Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
New Policy
Name
Fortigate Prod Captive Portal
Incoming Interface
Fortinet Prod (Fortigate Prod)
Outgoing Interface
wan1
Source
all
Destination
all
Schedule
always
Service
ALL
Action
ACCEPT
DENY
Inspection Mode
Flow-based
Proxy-based
Firewall / Network Options
NAT
IP Pool Configuration
Use Outgoing Interface Address
Use Dynamic IP Pool